Volume 18, Issue 42   Atari Online News, Etc.   November 4, 2016

=~=~=~=

A-ONE #1842   11/04/16

~ Shadow Brokers Hackers! ~ People Are Talking!   ~ Blizzard Voice Out!
~ Government IT Ancient! ~ Donkey Kong's Secrets! ~ Mac Google Ad Scam!
~ Star Control: Origins! ~ Facebook Advertisers! ~ Win 10 Update: 3D!

~ Zuckerberg Investigated ~ Win 10 Creators Update ~ Diablo 1 in Diablo 3

-* What To Know About Botnets! *-
-* Amateurs Caused Internet Meltdown? *-
-* U.S. Boosting Cyber Defenses for Election! *-

=~=~=~=

->From the Editor's Keyboard   "Saying it like it is!"
  """""""""""""""""""""""""""

In the immortal words of the late Harry Caray: Cubs Win! Cubs Win!
Cubs Win! I've been a Chicago Cubs fan since childhood; that's a
lot of years! Seeing that amazing 7th game of the World Series was
a memorable, if not nail-biting, event! The Cubs finally ended
the misery of Cubs fans worldwide, and finally, after 108 years,
brought a World Series championship back to Wrigley Field! Way to
go Cubbies!!

Well, history is about to be made in a few days! Yup, Election
Day is Tuesday. I don't know what more I can say about this
upcoming election that hasn't been said already. While the
candidates make their final pitches and toss around their final
insults at each other - it's time for Americans to make their
voices heard! Four more days!

Until next time...

=~=~=~=

     Apollo Team Announces Developing of Vampire Standalone
            Version To Run As Amiga and Atari ST

Hello, the Apollo team announces the developing of a standalone
version of the Vampire. They preview that it could be ready early
next year. But the availability of the ATARI version also depends
on if they can get support from the ATARI community because of
experience with the chipsets.

Source: http://www.apollo-core.com/knowledge.php?b=1&note=2723

Gunnar von Boehn
(Apollo Team Member)
25 Oct 2016 06:07

As many of you will know already, we are working right now on our
new card layout - which is optimized for mass production.

Based on the same features we will do both cards for all AMIGA

models as also new Standalones.

We expect the first bigger batch of these Standalone to receive
this year, and plan to be able to start normal sales beginning of
next year.

These standalones can be made both AMIGA and ATARI compatible.

In regards of AMIGA/ATARI chipset one could either instantiate
already existing and tested chipsets - or we could work together
on merging our SAGA chipset with an ATARI chipset.

As already announced some time ago - we will open source SAGA
when its done.

In regards of ATARI Testing and TOS hacking, and also Chipset
development - we would need some help - as none of us if
experienced here.

So if you are an ATARI expert and want to help to make this
happen then please contact us on IRC.

We hope that our standalone from its feature set can give a new
live to both retro platforms.

While we have no final price yet - our plan is to offer you the
highest possible value, most memory, and best performance for
the money.

                              =~=~=~=

->In This Week's Gaming Section - Blizzard Is Recreating Diablo 1 in Diablo 3!

   """"""""""""""""""""""""""""""   Blizzard Launches Blizzard Voice!
                                     Star Control Returns With Star Control: Origi
ns!

                                     And much more!

                              =~=~=~=

->A-ONE's Game Console Industry News   - The Latest Gaming News!
   """""""""""""""""""""""""""""""""""

           Blizzard Is Recreating Diablo 1 in Diablo 3,
                and the Necromancer Is Coming Too

Get ready for The Darkening of Tristram.

A big bit of Diablo news came out of BlizzCon today, as Blizzard

announced that the original Diablo is being recreated in Diablo 3.
The update, which will be a free event, will feature almost
everything you love about that great old game, from 16 levels and
four main bosses to a special graphics filter that will make the
graphics "pixelated and grainy," and even character movement
that's locked to eight directions.

"There will be many secrets to discover as well. If you love
Diablo, this anniversary event will be very nostalgic," chief
development officer Frank Pearce said during his presentation.

Pearce also revealed, not entirely surprisingly, that the
Necromancer class is coming to Diablo 3. The new class is a
"reimagining" of the Diablo 2 Necromancer, but will will wield at
least some of the same abilities, like Bone Spear and Corpse
Explosion.

"Necromancers can expect darker, more controlled gameplay
centered around the raw materials of life: blood and bone," the
Necromancer overview explains. "Grounded in a philosophical,
pragmatic approach to life and death, they re more like a
calculated conductor of the darkest arts. Deadly serious in
their practice, they are the experts of curses and reanimation
and their pets obey their every command.

The new class will be available as part of the Rise of the
Necromancer pack, which will also include an in-game pet, two
additional character slots, two extra stash tabs, a potrait
frame, pennant, banner, and banner sigil. A price hasn't been
set, but it will be released sometime in 2017.

Blizzard Launches Cross-game Voice Chat Service Blizzard Voice

Last October, Blizzard announced plans to add voice chat to its
multiplayer platform, which was then known as Battle.net. Now,
almost a year to the day since that announcement was made, the
company has rolled out the Blizzard Voice service to all users.

The functionality of Blizzard Voice is broadly similar to that
of Steam Voice Chat, according to a report from Engadget.
Players can talk to both friends and friends of friends whether
they re in-game or not, as long as the Blizzard Launcher
program is running.

That means that you can chat with your friend about their
Hearthstone draft while you re digging away at a raid in World
of Warcraft. Blizzard claims that its chat platform offers
 superior stability and extensive customization options in the
patch notes for the update that adds Voice capabilities to the
launcher.

However, the service omits one major feature that would have
benefited many players; it s not a traditional in-game chat
system. That means that you won t be able to use the Blizzard
Voice platform to strategize with other players as you re
preparing for a round of Overwatch, unless they re your friend,
or a friend-of-a-friend.

Some will be disappointed by this omission, while others would
perhaps prefer to keep their distance from the small, obnoxious
subset of players who will take advantage of any opportunity to
annoy their opponents. It s worth noting that Blizzard Voice
does allow users to mute or adjust the volume of others on an
individual basis.

While Blizzard Voice doesn t offer completely comprehensive chat
options just yet, there s every possibility that more features
will be added in the future. To gain access to this new
functionality, users should make sure that their installation of
Blizzard Launcher has been updated to the most recent version.

              Classic PC Franchise Star Control Returns
                    With Star Control: Origins

Developer Stardock revealed Star Control: Origins, its latest
game, and the first entry in the Star Control franchise since it
acquired the rights from Atari.

Described by Stardock as a "sci-fi action/adventure game" with
RPG elements, Star Control: Origins puts players in control of
"Earth s first interstellar starship."

Players navigate the ship through a "procedurally created
galaxy," contacting alien races, exploring planets, and fighting
"action packed battles."

The exploration and battle sequences take place over the backdrop
of a "complex intrigue that has the galaxy on the brink of
chaos."

Executive producer Brad Wardell said his team hopes fans of the
original "will like the direction we re taking," while
simultaneously "introducing a whole new generation" to the Star
Control franchise. In 2015, Stardock invited fans to help
determine the future of Star Control as a franchise.

Star Control 1, 2, and 3 were introduced in the early to
mid-'90s on PC. Stardock acquired the rights to the franchise
from Atari after Atari bankruptcy asset liquidation.

Star Control: Origins is coming to PC and consoles, with the PC
release scheduled for 2017. The game's "Founder's Program"
allows interested gamers to buy the first 3 games, now available
on the Star Control website, as well as pre-order the PC version
for $40 USD. Beta access, "mod tools, private journals, and more"
are included for members.

                              =~=~=~=

->A-ONE Gaming Online   -   Online Users Growl & Purr!

"""""""""""""""""""""

Bandit Gaming   Aventura Updates Classic Adventure for Sega Genesis

From Retro Gaming Magazine

The classic Adventure on the Atari 2600 was one of those games
that you either loved or hated. For many they loved it. It was
so different from what was available for the Atari, or any
console, back then. For me, I was too young to enjoy it early
on so I was not aware of its charms till the late 80 s but by
then I had already started gaming on the Nintendo Entertainment
System. Now, Devstar user landeel has taken it upon himself to
update the classic Adventure and port it to the Sega Genesis.
You can even play with Atari 2600 controllers if you want that
authentic feel. Time to enter the world of Aventura on your
Sega Genesis.

Adventure sets you off on a grand adventure to return the
Enchanted Chalice to the Golden Castle. Along your quest you
will encounter three dragons (red, green and yellow) and a bat
that is kind of a jerk. Within the kingdom are two other
castles, black and white, each with their own troubles and
treasures. That is what the manual says, or something similar
anyhow. What you actually see in Adventure is well, quite
different.

The graphics of Adventure are bare and Aventura is not doing
anything to change that. This is more of a straight port with
a couple of new game play modes to spice things up for hardcore
Adventure fans.

There are three game modes available in Aventura- Easy, Normal
and Random. There is also now a title screen, go technology!
Anyhow, the original game took Warren Robinette about a year to
layout and program. Aventura, using the original game as a
base, took about Landeel about three weeks to complete. Yeah,
yea I know, it is easier to follow a map made by someone else
than it is to make the map yourself.

Aventura is available on the Devster forums for free and is
another example BasiEgaXorz. Grab it, enjoy it. Need a Sega
Genesis to enjoy Aventura on? Grab one on Ebay.

        Atari and AtGames Announce Launch of Atari Flashback
            Classics Volume 1 and Volume 2 on Xbox One

Atari, one of the world's most recognized publishers and producers
of interactive entertainment, and AtGames, a leader in interactive
entertainment products, today announced the immediate availability
of their latest retro gaming releases, Atari Flashback Classics
Volume 1 and Atari Flashback Classics Volume 2 on Xbox One. Each
volume features 50 different classic Atari 2600 Video Computer

System (VCS) and arcade games. The two titles, which are now
available at leading retailers and online outlets, set the
standard for classic gaming on today's consoles.

"Atari Flashback Classics offers enhanced access to some of the
greatest titles in gaming history, bringing these beloved
favorites to a new generation of gamers," said Fred Chesnais,
Chief Executive Officer, Atari. "We are excited that the first
two entries in this critically acclaimed series are now
available to challenge and delight Xbox One gamers everywhere."

For the first time on Xbox One, players can experience Atari's
greatest hits with the benefit of today's technology, including
full 1080p high-definition, global leaderboards, online and
local multiplayer, and trophies and achievements. The intuitive
interface design delivers the responsive feel of the originals
on modern controllers. Featuring games like Asteroids,
Centipede, Missile Command, Tempest, Warlords, and many more,
each volume of Atari Flashback Classics combines the nostalgia
of the Atari 2600 and arcade legends with modern gaming
capabilities. Additionally, players can relive the glory days
with a massive library of original cabinet and box art.

"These two titles provide a modern showcase for many of the best
classic Atari games," said Dr. Ping-Kang Hsiung, CEO of AtGames.
"In our ongoing partnership with Atari, we are thrilled to help
bring these first two volumes to Xbox One gamers and look
forward to further developments in the series."

Atari Flashback Classics Volume 1 features the following titles:

3-D Tic-Tac-Toe (2600), Air-Sea Battle (2600), Backgammon (2600),
Basketball (2600), Black Widow (Arcade), Blackjack (2600),
Bowling (2600), Canyon Bomber (2600), Centipede (2600), Centipede
(Arcade), Circus Atari (2600), Combat (2600), Combat 2 (2600),
Desert Falcon (2600), Dodge 'Em (2600), Fatal Run (2600),
Football (2600), Home Run (2600), Human Cannonball (2600),
Liberator (Arcade), Lunar Lander (Arcade), Millipede (2600),
Millipede (Arcade), Miniature Golf (2600), Pong (Arcade), Quadrun
(2600), Radar Lock (2600), Realsports Boxing (2600), Realsports
Football (2600), Realsports Soccer (2600), Realsports Volleyball
(2600), Save Mary (2600), Slot Machine (2600), Slot Racers
(2600), Space Duel (Arcade), Sprint Master (2600), Star Raiders
(2600), Steeplechase (2600), Stunt Cycle (2600), Super Baseball
(2600), Super Football (2600), Swordquest: Earthworld (2600),
Swordquest: Fireworld (2600), Swordquest: Waterworld (2600),
Tempest (2600), Tempest (Arcade), Video Olympics (2600), Warlords
(2600), Warlords (Arcade), Yars' Revenge (2600)

Atari Flashback Classics Volume 2 features the following titles:

A Game of Concentration (2600), Adventure (2600), Asteroids
(2600), Asteroids (Arcade), Asteroids Deluxe (Arcade), Atari
Video Cube (2600), Basic Math (2600), Brain Games (2600),
Breakout (2600), Casino (2600), Championship Soccer (2600),
Checkers (2600) ,Chess (2600) ,Code Breaker (2600), Crystal
Castles (2600), Crystal Castles (Arcade), Demons to Diamonds
(2600), Double Dunk (2600), Flag Capture (2600), Golf (2600),
Gravitar (2600), Gravitar (Arcade), Hangman (2600), Haunted
House (2600), Major Havoc (Arcade), Maze Craze (2600), Missile

Command (2600), Missile Command (Arcade), Night Driver (2600),
Off the Wall (2600), Outlaw (2600), Race (2600), Realsports
Baseball (2600), Realsports Basketball (2600), Realsports
Tennis (2600), Red Baron (Arcade), Return to Haunted House
(2600), Secret Quest (2600), Sentinel (2600), Sky Diver (2600),
Spacewar (2600), Sprint (Arcade), Starship (2600), Stellar
Track (2600), Street Racer (2600), Sub Commander (2600), Super
Breakout (2600), Super Breakout (Arcade), Surround (2600),
Video Pinball (2600)

Developed by Code Mystics, Atari Flashback Classics is rated E
for Everyone. Each volume of Atari Flashback Classics carries
an SRP of $19.99 USD and is now available both digitally and
at major retailers.

 Miyamoto Spills Donkey Kong s Darkest Secrets, 35 Years Later

The best ideas for Donkey Kong were thought up when designer
Shigeru Miyamoto was fully nude. Just think on that for a while.

Done? OK.

In an interview with Nintendo s Creative Fellow posted today to
Nintendo s Japanese website, Miyamoto reaches back into his
memories of 35 years ago, when he created his seminal arcade hit
Donkey Kong. It was Miyamoto s first game as a director, it was
the origin of Mario, and it s one of the most important
videogames of all time. The home version of the game is also
getting a re-release, along with 29 other Nintendo Entertainment
System classics, via the plug-and-play NES Classic machine on
November 11.

Miyamoto has given countless interviews about Donkey Kong over
the course of his career, but in this chat, he spilled all
sorts of secrets I d never read before. It s long been known
that the game s protagonist was named Mr. Video and Jumpman
by Miyamoto, but that it was Nintendo s American branch that
christened him Mario due to his resemblance to their landlord,
Mario Segale. But did you know that Donkey Kong was supposed to
have human voice samples? Or that Nintendo had a company bathtub?
Here are the new secrets of Donkey Kong revealed, perhaps for the
first time, today.

Miyamoto didn t work on the NES version of Donkey Kong, but he
did work on other games.

Donkey Kong was released for the arcade in 1981, but came out on
the Famicom, the Japanese version of the NES, in 1983. Miyamoto
had nothing to do with this version, he said. The porting of
arcade games to Famicom, we left in the hands of a different team.
In order to get the Famicom off to a good start, I was working on
the rest of the software lineup.

While only three games were available for Famicom on its launch
day, Miyamoto says the team hoped to have about 7 games available
in short order. I personally really wanted there to be a
Baseball game, and so I was working on that, as well as games

like Tennis and Golf. These simple sports games aren t listed in
any of Miyamoto s official gameographies, but he says he was
all in on their creation: I was directly in charge of the
character design and the game design.

In fact, any game on the Famicom is designed around Miyamoto s
low-level specs: The 8-bit systems could only pull from a palette
of 64 possible colors, and Miyamoto helped to hand-pick which
colors it would support, he said.

Miyamoto told his friends he was going to disappear, and spent
four or five solid months on Nintendo s property.

Miyamoto had to create Donkey Kong under intense time pressure.
Nintendo of America was sitting on many unsold cabinets of a
failed arcade game called Radarscope, and it needed a replacement
game immediately. Miyamoto knew he was going into intense crunch
time, and telephoned several of his friends, saying, You
probably won t hear from me for about two or three months. This
was about how long it took to create a full game in those days,
he said but in fact, Donkey Kong ended up taking about four or
five months.

 At the time, I was living in company-owned housing, just across
the river from the office, Miyamoto said. Living in company
dorms was not unusual for young, unmarried guys in Japan. So
every day, I was just going back and forth between the office
and the company housing. Thank goodness we had a company bathtub!

This even surprised the Nintendo employee conducting the
interview. There was a company bath? he said.

 Yes, Miyamoto replied. At that time, our office was in
Tobakaido, which also housed the hanafuda factory. Nintendo had
been a maker of hanafuda, traditional Japanese playing cards,
since 1889, and this was still a major part of its business in
1981. There was a water boiler that was used to make the
hanafuda, and the water from this boiler was also used for a
bathtub. The employees making the hanafuda could wash their
sweat away in the bath after work, and at night when nobody was
around, you could hang out there for a long time.

 It totally saved me, Miyamoto said of the bathtub. It was
really effective at letting me put my ideas in order.

Miyamoto used Nintendo of America s ideas sometimes, but fought
them when he thought he was right.

 At that time, while I was making Donkey Kong, the conversations
were all around how globalism is important and we should
think worldwide,' he said. We listened to a lot of Nintendo of
America s opinions, but not all of them.

 For example, for the game s title, I was trying to convey the
idea of stupid monkey,' he said. Donkey of course referred
to the animal, but the dictionary I used said that it had a
secondary meaning of idiot. Nintendo of America said that this
was not the case, and donkey didn t mean idiot.'

 Even though it was in the dictionary, the interviewer said.

They said it sounded like she was talking about seaweed. It s a
mystery, Miyamoto replied. But I just liked the sound of it,
so I decided to stand my ground on Donkey Kong. And within a
year, everyone was saying Donkey Kong with no hesitation.

Miyamoto thought the details of Donkey Kong s storyline would
make it clear that Mario was supposed to be in his twenties. He
was wrong.

Many people are surprised when they find out that the Mario
character is supposed to be just out of college, probably since
that giant moustache makes him look like your retired uncle. I
didn t think he was an old man, Miyamoto said. I thought he
was more like 24 to 26 years old. When you think of the story
Mario kept Donkey Kong locked up, so he escaped with his
girlfriend   he was a young guy, a bachelor. But of course, now
there are people who think he s around 40 years old.

 The lady stolen away by Donkey Kong was supposed to yell out,
 Help, Help! And when Mario jumped over a barrel, she was
supposed to yell, Nice!, complimenting him. But some people
within the company said, Doesn t the pronunciation sound a
little weird? So we tested it on a native English speaker, a
professor. They said it sounded like she was talking about
seaweed: Kelp, Kelp!'

 At that point in development, we couldn t fix it, Miyamoto
said. So we took out all of the voices. Help! was replaced
with Donkey Kong s growl, and Nice! was replaced with the
pi-ro-po-pon-pon! sound. It s really good that we went with
pi-ro-po-pon-pon. When you walk past an arcade and hear that
sound, it s really catchy. So even though we took out the
voices, it still had great results. From this experience, I
learned the importance of having good sound effects.

(And yes, that means that the official onomatopoeia for
Mario s jumping sound is pi-ro-po-pon-pon! Another secret.)

Coming back to the NES Classic version of Donkey Kong,, Miyamoto
understands that today s players probably won t find it as
appealing. It has a certain stiffness to it, he says. You
can t move around as freely. The texture is much different from
today s games.

Miyamoto learned to loosen up, he says, after this game. I was
pretty serious when I was making this, he says. For example:
If you were to fall from a height equal to your own body height,
you d probably break your foot, right? So in Donkey Kong, if
you fall 1.5 times Mario s height, you die. But later I thought,
isn t it better if you don t die from such a thing? So in Mario
Bros., even if you fall five times Mario s height, you don t
die.

 But still, please enjoy this very serious game in which you die
if you fall off a single platform, Miyamoto concluded.

=~=~=~=

Amateur Hackers Probably Caused Friday's
Internet Meltdown, Researchers Say

Some have worried that the massive cyberattack that disrupted the
Internet on Friday was the work of Russian government-backed
hackers, politically motivated hacktivists or sophisticated
cybercriminals. But researchers at cyber-intelligence firm
Flashpoint say the Internet meltdown may have been carried out by
amateurs who haunt a popular hacking forum.

Flashpoint helped Web service provider Dyn determine that hacked
Internet-connected devices were involved in the attack, which
stopped or slowed access to Twitter, Spotify, Amazon and other
sites.

If Flashpoint is right, the attack shows that even hobbyists can
cripple the Internet's fragile infrastructure. When asked about
Flashpoint's research, Dyn pointed to a blog post on its site
Wednesday that said it's "collaborating in an ongoing criminal
investigation of the attack and will not speculate regarding the
motivation or the identity of the attackers."

The code for the malware Mirai, which was used in Friday's
attack, was posted roughly a month ago on an online community
called HackForums.net by someone using the handle "Anna-Senpai,"
as first reported by security journalist Brian Krebs. The same
user is believed to be behind earlier attacks using Internet of
Things devices controlled by Mirai, which last month targeted
Krebs' website and a French cloud provider called OVH, according
to Flashpoint.

Once the code was let loose online, almost anyone could have used
it or tweaked it for their own purposes, said Ben Herzberg, a
security research manager at cybersecurity firm Imperva. But
Flashpoint said its assessment points to HackForums users. People
posting on the site regularly trade tips on malware, and some
users have created tools that can launch digital assaults similar
to the one that hit Dyn on Friday. Some even offer to carry out
cyberattacks for a price, according to Flashpoint.

The operators of the HackForums site did not immediately respond
to a request for comment on Flashpoint's assessment.

HackForums users frequently target video game networks as a way
to get attention and prove their skills, the cybersecurity firm
said. Members have been linked to the hacking group that claimed
responsibility for knocking the PlayStation and Xbox networks
offline on Christmas Day in 2014.

In a blog post, Flashpoint said it discovered that the

infrastructure used to attack Dyn was also used to target "a well-known video game company." A post on HackForums said the original target of Friday's attack was the PlayStation Network and that Dyn was essentially collateral damage. Sony did not immediately respond to a request for comment on that claim.

Those clues point to amateur hackers   commonly known in hacker circles as "script kiddies"   as the culprits behind the Friday attack, according to Flashpoint.

"The technical and social indicators of this attack align more closely with attacks from the [HackForums] community than the other type of actors that may be involved, such as higher-tier criminal actors, hacktivists, nation-states, and terrorist groups," the Flashpoint researchers wrote.

Other experts agree with Flashpoint's assessment.

"I think they are right. I don't believe the Friday attackers were financially or politically motivated," said Mikko Hypponen, chief research officer at cybersecurity firm F-Secure. "It was such an untargeted attack, it's hard to find a good motive for it. So, kids."

What You Need To Know About The Botnet That Broke The Internet

A wave of cyberattacks against a core internet service provider last week caused disruptions at major websites and marked the third time in the past month that criminals used a network of malware-infected devices to cause havoc.

The botnet known as Mirai has garnered considerable attention from the security community because it is the first comprised entirely of ordinary internet-connected home products such as your digital video recorder and web cameras.

Many experts see it as a harbinger of a new trend where malicious hackers could take advantage of security weaknesses in these so-called Internet of Things (IoT) devices to quickly build vast networks of zombie home machines   or botnets   for launching different kinds of attacks.

In last week's attack, for instance, hackers used the Mirai botnet to direct huge volumes of useless traffic at the internet performance firm Dyn. The distributed denial of service, or DDoS, attack caused critical systems to become overloaded   and created big problems for Netflix, Spotify, Amazon, Paypal and numerous others Dyn customers.

"Last week's unprecedented DDoS attacks are only a preview of what is yet to come," warns Jeremiah Grossman, chief of security strategy at SentinelOne. With more than 20 billion "things" that will be connected to the Internet by 2020, the volume of devices that can be used in these attacks will be staggering, Mr. Grossman says. "Left unprotected, they have the potential to take down significant parts of the Internet."

Here's what you need to know about botnets such as Mirai and why they are the source of such concern:

Mirai is software that attackers use to build malicious networks from vulnerable IoT products. People can use it to constantly scan the internet for routers, DVRs, and other internet-connected products that are protected only by the generic usernames and passwords the products shipped with from the manufacturer. The software infects vulnerable systems and turns them into remotely controllable "bots" or machines that can be commandeered at will to do an attacker s bidding.

A malware-infected fridge or webcam, for instance, could also give attackers a way to break into other devices in your home network like your PC.

Mirai first surfaced in the days following a DDoS attack on the website of security blogger Brian Krebs in late September. The attack generated more than 600 gigabits of traffic per second, which was larger by several magnitudes than anything ever seen on the Internet till that point.

It was the first known instance where someone had used an IoT botnet to launch an attack of this scale. Mr. Krebs says that an analysis of the attack shows that tens of thousands of compromised home routers, DVRs, and IP cameras were used to launch the attack against his site. The attack on Krebs was quickly followed by an even larger 1 terabit per second attack on a French Internet Service Provider.

Shortly after the attacks, a cybercriminal using the handle "Anna-senpai" publicly released the code that was used to build the botnet. As Mr. Krebs noted at the time, the move virtually guarantees "that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders and other easily hackable devices."

Hardly. Mirai is one of at least two known malware families that are being used to assemble IoT based botnets, Mr. Krebs says. The other is called "Bashlight" and functions very much like Mirai. More than 1 million IoT devices are already believed infected with Bashlight, which means that those systems can be used any time to launch attacks like the ones on Dyn and Krebs.

Both of these are just early examples of software designed to take advantage of vulnerable IoT products. Attackers can build similar tools to take advantage of them in myriad other ways.

At least for the moment, IoT botnets are a lot easier to assemble than botnets compromised of malware-infected personal computers.

Typically, criminals looking to build a botnet have to find a way to infect tens of thousands of PCs with malware. In order to do this, they first have to send spam emails or phishing emails with malicious attachments, find a way to get past antivirus and antimalware tools and hope that enough recipients click on the attachments so their systems are infected.

In contrast, IoT devices are far easier to break into. And criminals can build much bigger botnets simply because of the

larger number of devices that are available to exploit.

A vast majority of ordinary home products connected to the
Internet are protected only with stock passwords. Security firm
ESET along with the National Cyber Security Alliance recently
surveyed about 1,530 US consumers on their use of IoT products.

Nearly 80 percent had seven or more devices connected to their
home router but only 30 percent had changed the password from the
factory default before connecting it to the Internet. Another
20 percent couldn t remember of they had.

To find vulnerable IoT devices, all an attacker needs to do is
use an internet scanning tool, like Shodan, to search for
specific IoT products and see which ones of them use a default
username and password, says Justin Harvey, security consultant
to internet traffic monitoring firm Gigamon.

"What makes them even more dangerous, is that many use a
protocol to 'announce' themselves to their home network," Mr.
Harvey says. The products then request the home router   often
without your knowledge   to open up a door in the router so the
device is accessible from the web.

Not much, unfortunately, at least so far. Hardware makers
rushing to get products out the door have paid far less attention
to ensuring their technologies can t be misused than software
makers. Few products for example are designed for easy patching
or security updates against a known security issue.

Many consumers are already uneasy with the trend. More than
40 percent of Americans in the ESET survey said they were not
confident that their IoT devices were safe. More than half said
they were discouraged from buying such systems because of
cybersecurity concerns

"Mirai must become the wake up call for the hardware industry,"
says Michael Sutton, chief information security officer at
ZScaler. "Hardware vendors simply haven't been forced to climb
the security learning curve the way that software vendors were
forced to. That's about to change."

Simply changing the default username and password on the devices
you connect to the Internet can go a long way in reducing
exposure. Figuring out how to do it, though, can be a little
trickier than changing the password on your bank accounts or
social media accounts, admits Stephen Cobb, senior security
researcher at ESET.

"In some cases, firmware needs to be updated, which can be a very
different process from a software update," Mr. Cobb says. "Often
you have to go looking for router and home device updates   they
are not routinely pushed to you the way that Microsoft and Apple
push Windows or Mac OS updates."

You can also use this IoT Scanner from security vendor BullGuard
to quickly check if the connected devices in your home are
publicly exposed on Shodan.

The Mirai attacks have stirred talk about the need for

regulations that would hold IoT device makers more accountable
for securing their products. The attacks this week prompted
Sen. Mark Warner (D) of Virginia to send a detailed questionnaire
to the chairman of the Federal Communication Commission, Tom
Wheeler seeking information on the tools that are available and
need to be developed for protecting consumer IoT devices from
mass compromise. Among the questions is one that inquires about
the feasibility of ISPs simply denying network access to insecure
and improperly secured IoT products.

                    U.S. Boosting Cyber Defenses,
                 But Not Police Presence, for Election

Federal and state authorities are beefing up cyber defenses
against potential electronic attacks on voting systems ahead of
U.S. elections on November 8, but taking few new steps to guard
against possible civil unrest or violence.

The threat of computer hacking and the potential for violent
clashes is darkening an already rancorous presidential race
between Democrat Hillary Clinton and Republican Donald Trump,
amid fears that Russia or other actors could spread political
misinformation online or perhaps tamper with voting.

To counter the cyber threat, all but two U.S. states have
accepted help from the U.S. Department of Homeland Security (DHS)
to probe and scan voter registration and election systems for
vulnerabilities, a department official told Reuters.

Ohio has asked a cyber protection unit of the National Guard, a
reserve force within the U.S. military, for assistance to
protect the state's systems.

On Thursday, Arizona Secretary of State Michele Reagan and her
cyber security team met with officials from the Federal Bureau
of Investigation (FBI) and the DHS, in addition to state-level
agencies, to discuss cyber threats, said Matt Roberts, a
spokesman for Reagan.

    Cyber security experts and U.S. officials say chances that a
hack could alter election outcomes are remote, in part because
voting machines are typically not connected to the internet.

But the FBI sent a flash alert in August to states after
detecting breaches in voter registration databases in Arizona
and Illinois.

Unidentified intelligence officials told NBC News on Thursday
that there is no specific warning about an Election Day attack,
but they remain concerned that hackers from Russia or elsewhere
may try to disrupt the process, likely by spreading
misinformation by manipulating social media sites such as
Facebook and Twitter.

DHS cyber security experts plan to hold a media briefing on
Friday to discuss the agency s efforts with states to boost the
security of their voting and election systems.

The potential for violence around the election has loomed in the background of the campaign for months. Armed groups around the country have pledged in unprecedented numbers to monitor voting sites for signs of election fraud.

Voter intimidation reported at polling sites so far prompted Democrats to accuse Trump of a "campaign of vigilante voter intimidation" in four states on Monday.

But local authorities surveyed by Reuters on Thursday in five states - Ohio, Pennsylvania, Arizona, Wisconsin and Florida - said they were not increasing election-related law enforcement personnel or resources above 2012 levels.

The FBI, which designates one special agent from each of its 56 field offices for election crime matters, has not increased its numbers or given staff additional training this year, said an FBI spokeswoman.

There has been no "substantive change" in the number of personnel deployed by the rest of the Justice Department, which designates Assistant U.S. Attorneys and federal prosecutors within the agency's Public Integrity Section to handle election crimes, according to a spokesman.

Jim Pasco, executive director of the Fraternal Order of Police, which represents hundreds of thousands of U.S. officers, said cops are taking the same security measures they would take for any large event. He said he expects the vows by militias to monitor the polls to be "a lot of talk, little action."

Civil rights groups said deploying more police officers to the polls can actually intimidate voters.

 The presence of law enforcement can have a chilling effect on the electorate, said Kristen Clarke, president of the Lawyers Committee for Civil Rights Under Law, a watchdog group. That s something we want to discourage.

NSA-Hacking 'Shadow Brokers' Reveal Spy-Penetrated Networks

Happy Halloween?

The Shadow Brokers, a mysterious hacker group, released a new cache of files online on Halloween morning.

The group claimed its latest dump reveals the IP addresses, or network designations, of computer servers supposedly compromised by The Equation Group, a hacker outfit widely believed to be linked to the United States National Security Agency. The list allegedly catalogues hundreds of the NSA-linked group s cyber-espionage targets from the 2000s, including a number of email providers and universities in China as well as targets in countries such as Iran, Russia, Pakistan, India, and South Korea.

 TheShadowBrokers is having special trick or treat for

Amerikanskis tonight, the shadowy group wrote in characteristically ungrammatical English in a post on the blogging site Medium, before posting links to the leaked files. The password to unlock them was payus.

Security experts noted the information leaked dated back to a decade ago. Some regarded the dump as a cry for attention on the part of Shadow Brokers, which have been trying to drum up interest in an online auction for Equation Group-linked hacking tools that it set up in August.

The earlier dump of hacking tools resulted in previously unknown exploits getting loose, causing networking equipment and firewall makers like, Fortinet, Juniper Networks, and the Chinese firm Topsec scrambling to issue patches for their devices.

This is being equation group pitchimpair (redirector) keys, many missions into your networks is/was coming from these ip addresses, the Shadow Brokers author wrote, referring to a hacking tool PITCHIMPAIR that supposedly compromised devices and converted them into staging grounds for launching further attacks. The cache also included systems targeted by the spy tool Intonation.

Matt Swann, a principal engineering manager at Microsoft, compiled the dumped data into an Excel spreadsheet. The document showed that the targets ran operating systems such as Sun Solaris, FreeBSD, and Linux.

The dump also referenced other hacking tools dubbed Dewdrop, Incision, Jackladder, Orangutan, Patchicillin, Reticulum, Sidetrack, and Stoicsurgeon about which little is known.

The Shadow Brokers author took the opportunity to rant about American spy agencies, media organizations, and the U.S. presidential election before asking for more bids in the aforementioned NSA-linked spy tools auction. At press time, the auction had raised just over 2 Bitcoins (about $1,400) in a total of 69 bids.

The Shadow Brokers previously said that the auction would end when we feel it is time to end, and the alleged loot would go to the highest bidder. The group said it would not reimburse losers.

How bad do you want it to get? the author said. When you are ready to make the bleeding stop, payus, so we can move onto the next game. The game where you try to catch us cashing out! Swag us out!

The latest file dump comes months after law enforcement arrested Harold Thomas Martin III, an NSA contractor who worked for Booz Allen Hamilton and whom some suspect might be tied to the Shadow Brokers leak. Martin allegedly stole 50 terabytes of data from the NSA and is awaiting trial.

Is Facebook Enabling Advertisers To Discriminate by Race?

Facebook s comment on troubling ad practice raises questions.

Facebook is about to have yet another, very uncomfortable
conversation about race.

A new story from the investigative journalism outfit,
ProPublica, has revealed that the company not only allows
advertisers to target users by specific attributes, they also let
them eliminate users on the basis of race. At best, the practice
is alarming, and at worst, illegal. Imagine if, during the Jim
Crow era, a newspaper offered advertisers the option of placing
ads only in copies that went to white readers, their report
begins.

Imagine indeed. From the story:

    The ubiquitous social network not only allows advertisers to
target users by their interests or background, it also gives
advertisers the ability to exclude specific groups it calls
 Ethnic Affinities. Ads that exclude people based on race, gender
and other sensitive factors are prohibited by federal law in
housing and employment.

ProPublica further drives their point home by successfully
purchasing an ad via the Facebook ad portal targeted to people
looking for housing but eliminating black, Asian and Hispanic
users. Not only is this potentially a legal issue, it feels like
a digital continuation of the redlining and similar practices
that have historically prevented people of color from
homeownership, financing, and employment.

Facebook s business model depends on advertising. To that end,
they give advertisers the ability to target users to an
exceptional degree of specificity. Not only do they collect an
extraordinary amount of data about people based on their activity
on the platform, they also enhance their databases with
information they purchase from data brokers about offline
behaviors as well.

Ultimately, people can be categorized in nearly 50,000 different
ways. The company told ProPublica that they re vigilant about
preventing discrimination or abuse on their ad platform and that
exclusion is an important way that advertisers can test the
effectiveness of ad copy, for example. But this episode will be
hard to explain away.

If nothing else, this report should raise yet again important
questions about how the algorithms that increasingly define our
lives are shaping the world in unseen ways. With all their data
and predictive analytics at their fingertips, how could Facebook
not have seen this coming?

Facebook s public relations firms, The Outcast Agency, sent a
statement in which it defended Facebook s advertising practice,
saying it is a way to ensure that ads can be tailored to a
particular audience and that they take enforcement action if they
find a problematic advertisement.

They also provided a screen shot of the ad ProPublica placed in

the story, which was to promote a ProPublica event, ironically about illegal real estate practices. But, the ad could just as easily have been for an event subtly hoping to attract only white potential renters or home-buyers. Did the ad approval process work in this instance? I m not sure they ve made their case. Stay tuned for more reporting on this.

The Facebook statement:

We are committed to providing people with quality ad experiences, which includes helping people see messages that are both relevant to the cultural communities they are interested in and have content that reflects or represents their communities not just generic content that s targeted to mass audiences. We believe that multicultural advertising should be a tool for empowerment. We take a strong stand against advertisers misusing our platform: our policies prohibit using our targeting options to discriminate, and they require compliance with the law. We take prompt enforcement action when we determine that ads violate our policies.

When World Cup 2014 became a big focus throughout the US Hispanic community, a business developed a campaign to reach people who had shown interest in that community in order to create a positive association between its brand and the world s most popular sport. This meant more relevant ads to those audiences about the World Cup.

All major brands have strategies to speak to different audiences with culturally relevant creative. Just for purposes of illustration, a car company will run creative for one of their vehicles, but will have one creative execution targeting the Hispanic affinity cluster in Spanish. They may create a different creative for the African American affinity cluster featuring black actors and stressing another insight that is specific to that group. All major brands do this because they know that audiences respond better to creative that speaks to them specifically. This is the case across all industries.

On exclusion targeting:? Marketers use this type of targeting to assess whether ads resonate more with certain audiences vs. others. For example, some audiences might click on Spanish-language ads for a World Cup sponsorship vs. other audiences might click more on the same ads in English, so the sponsor might run one campaign in English that excludes the Hispanic affinity group to see how well the campaign performs against running that ad campaign in Spanish. This is a common practice in the industry. We expressly prohibit discrimination and take prompt enforcement action when we determine that ads violate our policies.

Mark Zuckerberg Is Being Investigated by
German Prosecutors for Hate Speech on Facebook

We doubt Mark Zuckerberg is going to "like" this update.

On Nov. 4, Der Spiegel announced that prosecutors in Munich are

opening an investigation into Facebook founder Mark Zuckerberg and some fellow executives for possible criminal incitement and hate speech, as Facebook's policies may be in violation of Germany's hate speech laws. That's according to the criminal complaint filed by attorney Chan-jo Jun in Munich, Germany in September. At the time, a Facebook spokesperson said the complaint had no merit.

Jun filed an earlier complaint in Hamburg last year, but it went nowhere because the prosecutors, according to Der Spiegel, determined that Facebook was not under German jurisdiction. Prosecutors in Munich seem to indicate that German laws might just apply to the tech giant - or, at least, they are willing to see if they do.

Also under investigation are Chief Operating Officer Sheryl Sandberg and Facebook's European and German regional managers Richard Allan and Eva-Maria Kirschsieper.

Jun wants the the Facebook executives to be forced to remove from the site the postings he believes fall afoul of German law. He included in his filing 438 posts that allegedly contained racism, incitements to violence, and references to Nazis and the Holocaust. Facebook is certainly not the only social media platform to be criticized for its laissez-faire approach to hate speech - Twitter has been in the cross-hairs this election cycle - but there are only 4 million Twitter users in Germany. In February, Zuckerberg announced that he and Facebook would work with Germany to combat hate speech on his platform.

This is but the latest piece of bad news for Zuckerberg this week. Despite strong third quarter growth, Facebook CFO Dave Wehner warned investors Wednesday that future advertising revenue growth for the over $370-billion company will slow "meaningfully." That walloped the value of Zuckerberg's stake in the company, leaving him $3 billion poorer.

If there is a word to sum up such problems unique to the very rich and very powerful, it's sure to be a tongue-trippingly German creation.

Mac Owners: Watch Out For This Google Ad Scam

By now, you know not to click on suspicious-looking links, but did you know there's malicious software lurking behind Google's AdWords links?

A newly discovered malware campaign targeted Mac users looking to download the Chrome web browser, but instead gave them a ton of adware that peppered their screens with spam.

This scam was discovered by researchers at Cylance, an Irvine, CA-based antivirus firm, which disclosed the feature to Google on October 25 and published the news yesterday (Nov. 1). Google removed the malicious ads, but it's important to know how the scam works, because there is serious potential for others to use this attack vector to spread more dangerous malware.

Users who used Google.com to search for 'google chrome' received a legitimate link to download the browser in their results, but the AdWords result at the top of the page didn't direct users to the "www.google.com/chrome/" address it displayed. Instead, it redirects macOS users through a series of websites before opening the page "googlechromelive[.]com" which offers a free download of Google Chrome.

Clicking on that download button sent Mac users through another series of web pages before their browser automatically downloaded a malware file named 'FLVPlayer.dmg.' Running the application inside of that DMG package opened a webpage for MacPurifier, a 'scareware' program that tells users their system is riddled with viruses and that they need to download more programs, that are likely also scams.

Running the FLCPlayer.dmg file also downloads an installer for FastPlayer, a media player program that fills your screen with ads.

What should you do?

    First of all, always pay attention to the addresses of the sites you open. Just because a link or ad looked safe doesn't mean the content it sends you to is legitimate. Hovering your mouse over the link should reveal the destination.
    If your Mac's screen is filled with ads and you're concerned that you've accidentally downloaded malware onto your system, download Malwarebytes Anti-Malware for Mac, (or for PC), which is trustworthy and should eradicate those evil apps.
    Any decent antivirus program should also fight off these malware threats, so here are our favorite options for Mac antivirus software.

Government Propping Up Outdated Atari-like IT

When I was a wee little tyke, I had a Sega Genesis. A competitor to the Super Nintendo Entertainment System, it gave me hours of love-hate battles with two-dimensional characters (double entendre intended). It also instilled in me the conviction that hedgehogs are preferable to plumbers tripping on mushrooms.

I digress. I mention this nearly 30-year-old console because it turns out it's more advanced than Pentagon tech that handles launching nuclear weapons. That is bad.

On Wednesday, the U.S. Government Accountability Office reported on how federal agencies spend about $80 billion annually of our money on the computer systems that run the government. This year, almost 70 percent of that, $55.9 billion, is going to
 non-provisioned operations and maintenance.

In other words, the bulk of IT spending is being wasted to prop up ancient systems that need to die. The Office of Management and Budget has urged federal agencies for years to implement
 provisioned IT services, meaning modern systems with an

emphasis on cloud computing. Instead, agencies are spending most
of their IT budgets to limp 30- to 50-year-old legacy systems
along for another year. A decade might as well be a century in
IT. Case in point, Microsoft doesn't even support a 2003 Windows
server still used by the National Weather Service.

And then there's our nuclear arsenal. The report explains that
the Department of Defense's Strategic Automated Command and
Control System that coordinates the operational functions of
the United States' nuclear forces, such as intercontinental
ballistic missiles, runs on an IBM Series/1 Computer from the
1970s. As you may have heard, the system still uses 8-inch floppy
disks, capacity 80 kilobytes each. A Genesis game cartridge can
hold 50 times that, while the GAO notes a flash drive can hold
millions of times more data. (The Genesis cartridge still has
style, though.)

DOD has told the GAO it is upgrading the system and the floppy
disks will be gone by end of 2017. That's great, but those disks
are just a symptom of the frightening, pervasive neglect of our
world-ending weaponry. For an off-color primer on our nuclear
disarray, Google the nuclear weapons segment from comedian John
Oliver. (We nearly annihilated Goldsboro this one time.)

But let's set aside the issue of nuclear IT. Problematic,
vulnerable legacy systems also afflict other core governmental
functions. The Department of Treasury and the Department of
Veterans Affairs rely on COBOL, a programming language from the
'50s and '60s. The Department of Transportation uses outdated,
costly-to-maintain software to catalog hazardous materials
incidents. The same is true of the customized financial
management software that the Department of Homeland Security
(including the US Coast Guard) uses. DHS has well-defined plans
to upgrade its old systems, the GAO notes, but that's
unfortunately more than can be said for some systems at Treasury,
Commerce, the VA and the State Department.

That means agencies have wasted billions of dollars, as GAO IT
expert David Powner told Congress this week, according to PBS,
and show few signs of stopping. The report shows an untenable
downward spiral where growing operating and maintenance costs
are cannibalizing evermore funds needed for true solutions.

The story continues. Republicans and Democrats agree there's a
problem, but are still debating the solution. There's
understandable fear of the devil we don't know.

The devil we know is pretty freaking bad, though. Hopefully
Congress will see that and help Uncle Sam run his nukes on
something that's not so painfully close to being an Atari. The
least they can do is get us up to a Playstation 1. Then we could
start Armageddon based off of CDs.

I mean, destroying the Earth and using floppy disks? I would just
be too embarrassed.

Microsoft s New Update Is All About 3D

Microsoft has announced a new update to Windows 10, and the big theme is 3D.

It s called Creators Update, and there are three main features: 3D capabilities for everyone; 4K gaming and in-game broadcasting; and enhanced connectivity for friends, family and fellow gamers.

One highlight is Paint 3D. You will now be able to capture 3D scans of real-world objects, then import them to your computer and edit, view and move them around in a completely 3D space. You can easily upload the images to Facebook and share them with your friends and family.

Microsoft says the Creators Update will be available to download free next spring.

The Windows 10 Creators Update Could Streamline Your Friendships

Take off the VR headset and stop fiddling with 3D onscreen objects: The most important part of Microsoft s upcoming Windows 10 Creators Update may be its attempt to keep you in touch with close friends.

Microsoft s introduction of this free Win 10 revision in New York Wednesday morning led off with visions of virtual reality, augmented reality and 3D interfaces. But the bit that seems more likely to change the Windows experience is a sharing shortcut with the somewhat regrettable name of MyPeople.

This part of the Creators Update due early next year but available in preview form this week to Windows Insider users targets a long-running problem of messaging overload.

As daily correspondence climbs, it gets harder to stay in touch with family and friends (plus bosses and other people with unusual leverage over your bank balance). Existing tools like address autocomplete can t cope with that scenario and can become a liability when mere acquaintances share first names with lifelong pals.

The MyPeople feature Microsoft showed off instead lets you designate your closest friends, then elevates your interaction with them via shortcuts in the Windows taskbar. To send them a photo or a document, just drag that onto their mug shot at the bottom right of the screen.

Those shortcuts also let you jump into conversations with those people instead of watching their chit-chat vanish in your notifications. Microsoft product manager Allison O Mahoney demonstrated this feature by switching from a Skype messaging chat with her husband to an e-mail thread with him and then back to Skype, all without leaving a dialog floating over his taskbar shortcut.

MyPeople will also tie into SMS relay from Windows and Android phones, a feature you can use today in Windows 10 s Anniversary

Update. (Android users need to install Microsoft s Cortana app first.) And you can send shoulder tap emoji between Win 10 machines   though that may only fuel the messaging overload MyPeople strives to solve.

It all sounds a bit like the VIPs feature in Apple s Mail   but operating on a systemwide basis, not confined to one app. It also evokes the recent-contacts list Google s Android puts atop sharing menus, except that Android populates that automatically from your latest conversations instead of letting you anoint best buddies.

The graphically-intense features that began Wednesday s event made for more compelling demos, but they will require more powerful hardware than MyPeople and may also appeal to smaller audiences.

3D not in the wearing-glasses sense, but in the context of playing with 3D models on screen should have the most mass-market relevance.

The idea is that instead of having to model 3D objects in specialized apps, you could generate them from real-world objects using smartphone camera apps, download them from Microsoft s new Remix 3D gallery or import creations from Microsoft s Minecraft game.

Then you can share them in e-mail, on Facebook or even in PowerPoint; even the humble Paint app gets a 3D revival in Creators Update.

None of these features is new, but having a desktop operating system spotlight them should get more people interested.

VR has also struggled for mass-market relevance beyond 360 videos on Facebook or YouTube. Microsoft s HoloLens has drawn praise for its ability to overlay VR content on a view of the real world around you, but it s also a $3,000 purchase.

Windows 10 Creators Update, however, will support virtual-reality output to an upcoming line of VR headsets, starting at $299, from Acer, Asus, Dell, HP and Lenovo.

That update will also bring such new gaming features as easy broadcasting of a game and the ability to create custom multiplayer tournaments. Since I would only broadcast my performance in a game for comedic effect, I will leave it to others to judge their worth.

Feedback from Windows 10 users and Windows 7 holdouts who time spent in this software suggest other key areas for improvement. Alas, Wednesday s event had nothing to say about them.

The easiest fix should be the inexplicable lack of support for multiple time zones in Windows 10 s Calendar app. It s as if it s 2010 again and we re all puzzled by Google Calendar making us add or subtract hours to get transcontinental flight times correct   but Google fixed things by the end of that year. Get with it, Microsoft.

Addressing privacy concerns won t be so easy. Win 10 s
 telemetry helps Microsoft fix glitches by reporting when apps
crash, but its default settings can also result in snippets of
documents getting sent to Microsoft after a program bombs out
and generates a bug report. Win 10 s setup glosses over that
finer point in a glib Express Setup dialog which helps cede
the field of privacy-optimized Google alternatives to Apple.

The hardest fix may be basic reliability. Win 10 s Anniversary
Update got a thumbs-down from users with external webcams after
that August release stopped many of those devices from working.
It s disturbing that Win 10 s wide pre-release circulation
among Windows Insiders didn t get this problem to Microsoft s
attention early on; it will be more disturbing if Creators
Update ships with a bug of comparable magnitude.

=~=~=~=